Committee Draft **ISO/IEC CD 15292**	
Date: **2000-01-03**	Reference number: ISO/IEC JTC 1/SC 27 **N 2451**
Supersedes document SC 27 N 2335	

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2000-04-03** Please return all votes and comments in electronic form directly to the SC 27 Secretariat by the due date indicated.

ISO/IEC CD 15292

Title: Information technology – Security techniques – Protection profile registration procedures

Project: 1.27.20

Introductory note:
In accordance with resolution 6 (SC 27 N 2466) of the 11th SC 27 plenary meeting in Columbia, USA, October 1999, the attached document is hereby being submitted for a three-month CD letter ballot closing

April 3, 2000

Medium: Server

No. of pages. : 16

Address Reply to:

Secretariat, ISO/IEC JTC 1/SC 27 -
DIN Deutsches Institut fuer Normung e.V., Burggrafenstr. 6, 10772 Berlin , Germany
Telephone: + 49 2601-2652; Facsimile: + 49 2601-1723; E-Mail: passia@ni.din.de,
HTTP://www.din.de/ni/sc27

Vote on Committee Draft ISO/IEC CD 15292

Date of circulation: **2000-01-03** Closing date: **2000-04-03**	Reference number ISO/IEC JTC 1/SC 27 **N 2451**

ISO/JTC 1/SC 27 Information technology – Security techniques Secretariat: Germany (DIN)	Circulated to P-members of the committee for voting Please return all votes and comments in electronic form directly to the SC 27 Secretariat by the due date indicated.
ISO/IEC CD 15292 Title: Information technology – Security techniques – Protection profile registration procedures Project: 1.27.20	

Vote:

_____	APPROVAL OF THE DRAFT AS PRESENTED
_____	APPROVAL OF THE DRAFT WITH COMMENTS AS GIVEN ON THE ATTACHED
___	general:
___	technical:
___	editorial:
_____	DISAPPROVAL OF THE DRAFT FOR REASONS ON THE ATTACHED
___	Acceptance of these reasons and appropriate changes in the text will change our vote to approval
_____	ABSTENTION (FOR REASONS BELOW):

P-member voting:

National Body (Acronym)

Date:

CCYY-MM-DD

Submitted by:

Name

Address Reply to:
Secretariat, ISO/IEC JTC 1/SC 27- DIN Deutsches Institut für Normung e.V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-Mail: passia@ni.din.de; HTTP://www.din.de/ni/sc27

Protection Profile registration procedures

(CD 15292)

Project JTC 1.27.20

- Committee Draft -

First Committee Draft
31 December 1999

Project Editor:

Dr. M. J. Nash
Gamma Secure Systems Limited
Diamond House, 149 Frimley Road
Camberley, Surrey, GB-GU15 2PS
United Kingdom
E-mail: mnash@gammassl.co.uk

Contents

Information technology - Security techniques - Protection Profile registration procedures

1 Scope

This International Standard defines the procedures to be applied by the JTC 1 Registration Authority appointed by the ISO and IEC councils to maintain a register of Protection Profiles and packages for the purposes of IT security evaluation.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated documents, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 15408-1, *Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.*

ISO 15408-2, *Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functionality requirements.*

ISO 15408-3, *Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements.*

JTC 1 Directives, Fourth Edition, 1998-08-31.

ISO/IEC/ITU ITSIG Guide for the use of IT in the development and delivery of standards.

3 Terms and definitions

3.1
applicant
an entity (organisation, individual etc.) which requests the assignment of a register entry and entry label

3.2
certificate
a declaration by an independent authority operating in accordance with ISO Guide 58, confirming that an evaluation pass statement is valid

3.3
entry label
the naming information that identifies a registered PP or package uniquely

3.4

evaluation pass statement
a statement issued by an organisation that performs evaluations against ISO/IEC 15408 confirming that a PP has successfully passed assessment against the evaluation criteria given in clause 4 of Part 3 of that International Standard

3.5
JTC 1 Registration Authority
an organisation appointed by the ISO and IEC councils to register objects in accordance with a JTC 1 procedural Standard

3.6
package
a reusable set of either functional or assurance components combined together to satisfy a set of identified security objectives (from ISO/IEC 15408-1)

3.7
Protection Profile
an implementation-independent set of security requirements for a category of IT products or systems that meet specific consumer needs (adapted from ISO/IEC 15408-1)

3.8
register
a set of files (electronic, or a combination of electronic and paper) containing entry labels and their associated definitions and related information

3.9
register entry
the information within a register relating to a specific PP or package

3.10
registration
the process of assigning a register entry

3.11
Security Target
A set of security requirements and specifications to be used as the basis for evaluation of an identified IT product or system (adapted from ISO/IEC 15408-1)

3.12
sponsor
an entity (organisation, individual etc.) responsible for the definition of a register entry

4 Abbreviations

ITTF	Information Technology Task Force (of ISO/IEC)
PP	Protection Profile
RA	Registration Authority
RG-RA	JTC 1 Rapporteur Group on Registration Authorities
SC	JTC 1 Subcommittee
ST	Security Target

5 Technical Specifications

5.1 Entry label

Every PP or package registered in accordance with this International Standard shall have an entry label assigned by the JTC 1 RA that uniquely identifies that PP or package within the register. The entry label shall be made up of the following elements, separated by dashes:

- Entry Type
- Registration Year
- Registration Number.

The Entry Type shall be PP for a protection profile, AP for an assurance package or FP for a functional package.

The Registration Year shall be the four digit representation of the year when the entry was registered.

The Registration Number shall be a four digit sequentially assigned identification number, starting each year from 0001.

EXAMPLE PP-2000-0001.

5.2 Technical definition (within a register entry)

Every application for registration of a PP submitted for registration in accordance with this International Standard shall include a technical definition of the PP structured in accordance with Annex B of ISO/IEC 15408-1.

Every application for registration of a functional or assurance package submitted for registration in accordance with this International Standard shall include a technical definition of the package. This definition shall contain:

- a package overview that summarises the package in narrative form
- a specification of a set of either functional or assurance components.

The package overview should be sufficiently detailed for a potential user of the package to determine whether the package is of interest. It should be understandable without reference to the component specifications.

Components for functional packages shall be selected from ISO/IEC 15408-2 or shall be constructed and structured in accordance with the specification requirements for functional components given within clause 2 of ISO/IEC 15408-2.

Components for assurance packages shall be selected from ISO/IEC 15408-3 or shall be constructed and structured in accordance with the specification requirements for assurance components given within subclause 2.1 of ISO/IEC 15408-3.

The technical definition of a package may contain other descriptive information that might be relevant to the author of a PP or ST wishing to use or reference the package. This information shall be structured in accordance with the specification rules given within Annexes B and C of ISO/IEC 15408-1.

6 The JTC 1 Registration Authority for PPs and packages

6.1 Appointment

The JTC 1 RA for PPs and packages shall be appointed by the ISO and IEC councils in accordance with the procedure for the appointment of JTC 1 Registration Authorities defined in the JTC 1 Directives.

6.2 Qualifications

Any organisation seeking appointment as the JTC 1 RA for PPs and packages shall demonstrate that it meets the qualifications required of JTC 1 RAs as defined in the JTC 1 Directives, with the following amendments:

- it shall confirm its agreement to function as an RA for a minimum of 5 years only;
- it shall confirm that it has sufficient equipment resources and communication facilities to operate an Internet web site in support of this International Standard;
- it shall confirm that on termination of its appointment, it will transfer its register and all supporting documentation at no cost to another organisation designated by the ISO and IEC councils.

6.3 Contract

The JTC 1 RA for PPs and packages shall operate under contract with the ITTF. Upon twelve-months notice, either the RA or the ITTF may terminate the contract.

6.4 Duties

The JTC 1 RA for PPs and packages shall:

- receive applications for the registration of PPs and packages;
- review applications for the registration of PPs and packages;
- assign unique entry labels to PP and packages added to the register;
- inform applicants for registration of the results of their applications;
- inform sponsors of the results of actions relating to their register entries;
- maintain an accurate register;
- make public access to complete details of all register entries available at no cost via the world wide web and provide printed details of register entries on demand, in return for payment of a fee if required;
- publish details of its fee structure, if it operates on such terms;
- handle all aspects of the registration process in accordance with good business practice;
- provide an annual summary report on its activities to JTC 1, ITTF and the SC responsible for this International Standard;

- adhere to the procedure for appeals contained within this International Standard;

- maintain a copy of the register in the English language;

- handle all correspondence relating to the register or register access in the English language, except by mutual agreement of the RA and the other party;

- produce guidance, practice and tutorial web pages and documents where applicable;

- indicate (e.g. on web pages and stationery) that it has been designated a JTC 1 RA in accordance with this International Standard by ISO/IEC.

7 Criteria for eligibility of applicants for registration

Any organisation or individual may submit an application for registration of a PP or package to the JTC 1 RA for PPs and packages.

8 Information to be included within an application for registration

An application for registration of a PP or package shall include:

- the name and contact details of the applicant. Contact details shall include both a postal or E-mail address and a telephone or facsimile number. If the applicant is an organisation, contact details shall include the name and title of a contact person within the organisation;

- the type of object submitted for registration. This shall be a PP, functional package or assurance package;

- a statement as to whether the PP or package is submitted for registration as a new entry or replacement entry. If the PP or package is submitted as a replacement entry, the entry labels of the existing register entries to be replaced shall be identified. The application shall include a statement from the sponsors of those entries confirming that if the replacement entry is accepted, they will agree to the linking of their existing entries to the replacement;

- a statement as to whether the PP or package is submitted for registration as being complete or incomplete;

- the technical definition of the new PP or package. If the PP or package is designated incomplete, sections of the technical definition may be marked as “to be defined later”. The technical definition shall not reference other PP or package specifications for definition purposes, whether registered or otherwise;

- a declaration that the applicant will act as the sponsor of the register entry for the minimum period applicable to the type of entry in question;

- a declaration that the specification of the PP or package submitted for registration does not contain secret, proprietary or non-publishable information;

- any initial fee required by the RA for consideration of the application;

An application for registration of a PP may also include:

- an evaluation pass statement or certificate for the PP in question, together with the name and contact details of the organisation that issued that statement or certificate.

Application for registration shall be made in the English language, except by mutual agreement between the applicant and the RA. The technical definition of the PP or package may be specified in any natural language, provided that the PP or package overview and the structure of the remainder of the definition are supplied in the language of the application for registration.

Versions of the technical definition in several natural languages may be supplied. However, one version shall be identified as the official version for the register entry and all other versions as informative translations.

An electronic copy of the technical definition shall be supplied with the application. This electronic copy shall use a file format and transport mechanism recommended for the exchange of electronic documents within the Guide for the use of IT in the development and delivery of standards.

9 Steps involved in review and response to an application

9.1 Initial processing

All applications for registration of PPs or packages in accordance with this International Standard shall be subjected to initial processing by the RA.

This process shall check that all required elements of the application are present, and in the opinion of the RA, adequate for further processing.

The RA shall either reject the application or assign the PP or package an entry label and enter the PP or package into the register with a status of “in validation”. The applicant shall be advised accordingly.

This process shall be completed within 14 days of receipt of the application.

9.2 Validation

The RA shall perform an editorial check of the format of the technical definition provided within the application for registration. All required sections shall be present, except for sections of incomplete entries marked as “to be defined later”. If information is missing, or presented in a format which is incompatible with the current version of ISO/IEC 15408, including relevant technical corrigenda or amendments published by the ITTF, the RA shall refer the issue or issues to the applicant for clarification or rectification. If the applicant cannot resolve omissions or inconsistencies within 14 days of receipt of notification of the issue, the PP or package shall fail validation.

If an evaluation pass statement or certificate is supplied, the RA shall contact the organisation that issued the statement or certificate and provide them with a copy of the application. The evaluating or certifying organisation shall be requested to confirm within one month that the technical definition of the PP as evaluated is identical to that as submitted for registration, and that the PP was awarded a pass statement. If the organisation cannot be contacted, does not reply, or does not offer the requested confirmation, the RA shall declare the statement or certificate not acceptable and advise the applicant accordingly.

If the application for registration identifies one or more existing register entries that are to be replaced, the RA shall contact the organisations that currently sponsor those entries and provide them with a copy

of the application and their statement agreeing to the linking of their entries as replaced. The sponsoring organisations shall be requested to confirm within one month the validity of these statements. If any organisation cannot be contacted, does not reply, or does not offer the requested confirmation, the RA shall declare the replacement linkage not accepted and advise the applicant accordingly.

The RA shall complete this validation, including any referrals that are necessary, within 3 months of receipt of the application. If the applicant has been unable to resolve an issue, the register entry shall then be given a status of “failed validation”. Otherwise the status shall become either “registered”, or in the case of a complete PP where an acceptable evaluation pass statement or certificate was supplied, “evaluated” or “certified” as appropriate. The routine review date shall be set to 36 months from the date of initial entry onto the register in the case of complete entries and 12 months in the case of incomplete entries.

NOTE Validation by the RA is restricted to the editorial and consistency checks defined above and does not include evaluation of the technical definition using ISO/IEC 15408. Only where an entry has “evaluated” or “certified” status is any assertion made concerning the technical accuracy of the register entry.

10 Criteria for rejection of applications for registration

An application for registration of a PP or package shall be rejected if:

- the applicant fails to pay any fee required by the RA;
- required elements of the application are missing;
- the application contains missing or incomplete information (except where expressly permitted by this International Standard);
- the application contains information designated secret, proprietary or non-publishable;
- the application contains incomprehensible information;
- the technical definition of the PP or package to be registered is not structured in accordance with the requirements of subclause 5.2 of this International Standard.

11 Operation of the register

11.1 Notification of obsolescent entries

The RA may be advised at any time by the sponsor of a complete register entry with “registered”, “evaluated” or “certified” status that the entry in question is consider unsuitable for future use on grounds of obsolescence. The register entry status shall be updated to “obsolescent”, and the routine review date shall be set to 18 months from the date of receipt of the advice.

11.2 Routine review of entries

On the routine review date for incomplete entries with a status of “registered”, and of complete entries with the status of “obsolescent”, their status shall become “retired”.

One month prior to the routine review date of entries with a status of “registered”, “evaluated” or “certified”, the RA shall contact the sponsor of the entry and ask the sponsor to confirm the entry. In the

case of a PP entry with a status of “evaluated” or “certified” where defect resolution notes are present that are not covered by the evaluation pass statement or certificate, the RA shall also request the sponsor to provide a new evaluation pass statement or certificate that takes the defects and associated resolution actions into account. The RA may also require the payment of a further fee for continuing registration.

If the sponsor of the entry advises that they do not wish to continue registration, or does not reply within one month of the revalidation request, or does not pay any required fee, the status of the register entry shall become “obsolescent”. If a new evaluation pass statement or certificate is requested, but is not supplied by the sponsor, the status of the entry shall be downgraded to “registered”. The routine review date shall be updated to be 18 months from the date of review for entries now marked “obsolescent” and to be 36 months from the date of review in all other cases.

11.3 Defect notification

The RA may be advised at any time by any person of a claimed error, defect, inconsistency or ambiguity within a register entry. Upon receipt of such a report, the RA shall advise the sponsor of the register entry of the claimed defect.

If within one month the person reporting the claimed defect withdraws the notification, the register entry shall remain unchanged. Otherwise, the sponsor of the entry shall within that time period provide a defect resolution note describing the problem and providing a response. This may be to record that, in the opinion of the entry sponsor, no defect exists. The RA shall append the defect report and its resolution note to the technical definition within the register entry. The RA shall also send a copy of the resolution note to the person who reported the defect.

NOTE The sponsor of the register entry is encouraged to contact the person reporting the defect in order to reach a mutually agreeable response, but is not required to do so. There will be some types of defects that cannot be solved by means of a defect resolution note. In such cases, a replacement entry will need to be registered and the existing entry marked as obsolescent.

If no defect resolution note is provided by the sponsor within the required time, the status of the register entry shall become “obsolescent”. The defect report shall be appended to the technical definition within the register entry and the date of next routine review set to 18 months from the date of the change of status.

If ISO/IEC 15408 is amended, or found to be defective, then register entries can become inconsistent or defective when compared against the revised criteria. Such defects shall be recorded if reported.

11.4 Other requests for update of entries

The RA may be advised at any time by the sponsor of a register entry of changed contact details for the sponsor. Within one week of receipt, the RA shall update the register entry accordingly.

At any time the sponsor of a register entry may request that sponsorship of the entry is transferred to another person or organisation. Such requests shall include a statement from the proposed new sponsor accepting the transfer of sponsorship. Within one week of receipt, the RA shall update the register entry accordingly, advising both new and old sponsors that the change has been made.

The RA may receive at any time from the sponsor of a complete PP register entry with “registered” status an evaluation pass statement or certificate for the entry in question. Upon receipt, the evaluating or certifying organisation shall be requested to confirm within one month that the PP was awarded a pass statement, and that the technical definition of the PP as evaluated is identical to that registered. If the organisation cannot be contacted, does not reply, or does not offer the requested confirmation, the RA shall declare the statement or certificate not acceptable and advise the applicant that the status of

"registered" remains unchanged. Otherwise the status of the entry shall be updated to "evaluated" or "certified", as appropriate.

The RA may be advised at any time by the organisation that issued an evaluation pass statement or certificate referenced in a register entry with "evaluated" or "certified" status that the statement or certificate in question has been withdrawn. Upon receipt of such notification, the status of the register entry shall be downgraded to "registered".

None of the register entry changes permitted by this subclause shall change the date of next routine review for the entry.

11.5 Deletion of register entries

Register entries once allocated an entry label shall never be deleted from the register.

NOTE Entries that are no longer in active use can be distinguished by their "retired" status.

12 Maintenance of the register

The RA shall take appropriate measures to ensure that accuracy of the information within the register is maintained, information within the register is publicly accessible without unreasonable delay, and that adequate backup and recovery measures exist to protect the register.

These measures shall be specified in the contract between the RA and ITTF.

13 Confidentiality of information held within the register

Register entries shall not contain secret, proprietary or non-publishable material. All information within all register entries shall be made publicly available by the RA.

14 Publication of the register

The JTC 1 RA appointed under the terms of this International Standard shall maintain a register of all PPs and packages that it has accepted for registration. The register shall be maintained and published in the English language. Informative translations of the register or individual register entries may, if the RA wishes, be provided in other languages.

The register entry for each PP or package shall contain at least the following information:

- The entry label for the entry;
- The type of object registered, either "PP", "functional package" or "assurance package";
- Whether the entry is a new or replacement entry;
- Whether the entry is designated complete or incomplete;
- The status of the entry, one of "in validation", "failed validation", "registered", "evaluated", "certified", "obsolescent", or "retired";
- The date of original acceptance of the entry;

- The date of the last change to the entry;
- The date for the next routine review of the entry;
- The name and contact details of the current sponsor of the entry;
- The name and contact details of the original applicant for registration;
- Where the status of the entry is “evaluated” or “certified”, the name and contact details of the organisation that issued the evaluation pass statement or certificate;
- The technical definition of the PP or package, together with any applicable defect reports and defect resolution notes;
- The version of ISO/IEC 15408 against which the entry was validated, including any relevant technical corrigenda or amendments published by the ITTF that were taken into account;
- The entry labels of any entries replaced by the entry;
- The entry label of any entry replacing this entry.

The section headings and other structural information of the technical definition of the PP or package shall be in English using the titles defined in ISO/IEC 15408. Sections marked as “to be defined later” shall be identified in English. Other aspects of the technical definition of the PP or package may be written in a natural language other than English.

The RA shall make access available at no cost to all the information identified above for all register entries, via the world wide web.

Upon request, and upon payment of a fee if applicable, the RA shall provide printed details of one or more register entries containing all the information identified above.

Upon request, and upon payment of a fee if applicable, the RA shall provide a printed copy of the complete register.

15 Appeals procedure

Editors note: the contents of this clause must be agreed by the JTC 1 Rapporteur Group on Registration Authorities (RG-RA) and with candidates for the Registration Authority. The following text is offered for their consideration.

In the event of a dispute between an applicant for registration or the sponsor of a register entry and the RA, the applicant or sponsor shall contact the chief executive of the RA, setting out the grounds for disagreement and the action requested of the RA.

The chief executive of the RA shall consider the issue in question, and within one month issue a decision to the complainant and to the operational staff of the RA.

If the complainant is not satisfied by the decision of the chief executive, the complainant shall within one month appeal formally to the chief executive by letter, setting out the grounds for non-acceptance of the decision.

The chief executive shall consider the grounds for appeal, and within one month by letter confirm or revise his or her previous decision.

If the complainant is not satisfied by the appeal decision of the chief executive, the complainant shall within one month write to the secretariat of the JTC 1 subcommittee responsible for this International Standard, setting out the grounds of the dispute, the decision of the chief executive of the RA and the grounds for non-acceptance of that decision.

The secretariat shall request the issue to be considered by the SC responsible for this International Standard. Upon such a request, within two years the relevant SC shall by resolution provide a decision to the issue in question, which shall thenceforth be binding upon both the complainant and the RA.

Annex A
(informative)

Benefits of registration

The benefits of registration of PPs and packages are:

- as a shorthand way to publicise common security requirements, to assist users to compare the security claims of competing products or systems;

- as a way that industry sector or product vendor associations can specify minimum standards for security functionality and assurance, as a public guide to prospective product manufacturers developing new commercial products;

- as a public domain basis for purchasers to specify security requirements for incorporation within multiple acquisition specifications;

- where a PP has been evaluated, developers of Targets of Evaluation (TOEs) incorporating that PP will benefit by a reduction in cost, risk and complexity of evaluation, since the PP portion of the work will not need to be repeated.